

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-134302

(43)Date of publication of application : 21.05.1999

(51)Int.Cl.

G06F 15/00

G06F 1/00

G06T 7/00

G06K 17/00

G06K 19/10

(21)Application number : 09-300176

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 31.10.1997

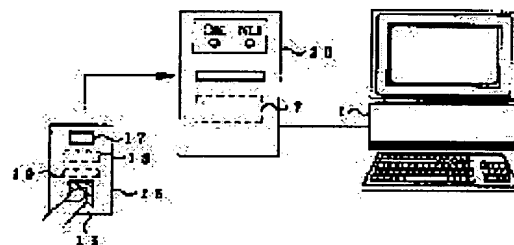
(72)Inventor : KUBO TAKEHIRO

(54) ACCESS CONTROLLER FOR TERMINAL, AND AUTHENTICATION CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an authentication card from being used by an illegal user and to eliminate the need to change settings of readers connected to individual terminals even when users increase or decrease in number by sending terminal use permission information when a fingerprint of a user matches fingerprint information registered in an authentication device.

SOLUTION: The user after pressing his or her fingerprint against a card type authentication device 15 inserts the side wherein a terminal use information entry unit 17 is built into a card reader 20. The card reader 20 reads the terminal user permission information out of the terminal use information entry unit 17. A terminal use permission information decision unit 7 built in the card reader 20 decides whether or not the read information read by the card reader 20 is correct. When the information is correct, information for allowing the terminal 1 to be used to the terminal 1. The terminal 1 receives the information sent from the terminal user permission information decision unit 7 and allows the user to use the terminal 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開平11-134302

(43) 公開日 平成11年(1999) 5月21日

(51) Int.Cl. ⁶	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 F
1/00	3 7 0	1/00 3 7 0 E
G 0 6 T 7/00		G 0 6 K 17/00 V
G 0 6 K 17/00		G 0 6 F 15/62 4 6 0
19/10		G 0 6 K 19/00 S

審査請求 未請求 請求項の数12 O L (全 11 頁)

(21) 出願番号 特願平9-300176

(22) 出願日 平成9年(1997)10月31日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 久保 剛弘

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

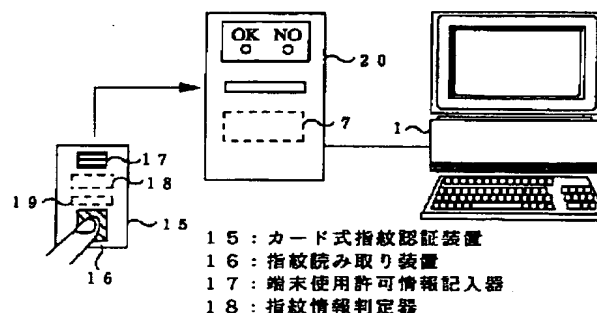
(74) 代理人 弁理士 宮田 金雄 (外2名)

(54) 【発明の名称】 端末のアクセス制御装置および認証カード

(57) 【要約】

【課題】 従来のアクセス制御方式は、端末に利用者のパスワードを打ち込む方法や磁気カードや集積回路を組み込んだカードを使用する方法や、利用者の指紋を利用する方法を用いていた。しかし、パスワードを打ち込む方法や磁気カードや集積回路を組み込んだカードを使用する方法では、パスワードや磁気カード、集積回路を組み込んだカードを不正な利用者によって利用される可能性があった。一方、利用者の指紋を利用する方法では、利用者の増減によって端末に接続されている全ての指紋認証装置の設定を変更する必要があった。

【解決手段】 カード式認証装置に組み込まれた端末使用許可情報を、登録された指紋情報と利用者の指紋が一致した場合に書き込むことによって、不正な利用者が利用することを防ぎ、又、利用者の増減があった場合にも、個々の端末に接続された読み取り装置の設定を変更せずに済むようにする。



【特許請求の範囲】

【請求項 1】 情報検索等を行う端末のアクセス制御装置において、カード読み取り装置に設けられ、端末使用許可情報を判定し、正しい情報であった場合、端末に使用許可情報を送信し、端末を使用可能にする端末使用許可情報判定器と、端末を使用しようとする際に、利用者自体の指紋と、予め登録してある指紋情報とが一致した場合に、端末使用許可情報を記録する認証カードと、上記認証カードに設けられ、利用者自体の指紋を読み取る指紋読み取り器と、上記認証カードに設けられ、読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記認証カードに電気を供給する電源と、端末に接続され、利用者が端末を利用しようとする場合、利用者が所持している上記認証カードが挿入され、その端末使用許可情報を読み取り、端末使用許可情報判定器に送信するカード読み取り装置とを備えたことを特徴とする端末のアクセス制御装置。

【請求項 2】 端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって、この認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、予め登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、複数の利用者の指紋情報が登録されたメモリとを備えたことを特徴とする認証カード。

【請求項 3】 端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって上記認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記読み取った指紋情報と登録された利用者の指紋情報とが不一致の場合不正利用された事を報知する報知手段とを備えたことを特徴とする認証カード。

【請求項 4】 上記報知手段はスピーカあるいは無線の送受信器で構成したことを特徴とする請求項 3 記載の認証カード。

【請求項 5】 利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と予め登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使

用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、内部電源と、外部から供給された電気によって上記内部電源を充電する充電器とを備えたことを特徴とする認証カード。

【請求項 6】 端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録するカード式認証装置と、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、内部電源と、内部電源に電気を供給する太陽電池とを備えたことを特徴とする認証カード。

【請求項 7】 端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって上記認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、内部電源と、認証カードを振動させることで発電し、上記内部電源に電気を供給する振動発電器を備えたことを特徴とする認証カード。

【請求項 8】 カード読み取り装置に設けられ、端末使用許可情報を判定し、正しい情報であった場合、端末に使用許可情報を送信し、端末を使用可能にする端末使用許可情報判定器と、端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードと、上記認証カードに設けられ、利用者自体の指紋を読み取る指紋読み取り器と、上記認証カードに設けられ、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記認証カードに設けられ、上記認証カードをカード読み取り装置に挿入した際、カード読み取り装置から電源を供給する外部電源器と、端末に接続され、利用者が所持している認証カードが挿入されたときその端末使用許可情報を読み取り、上記端末使用許可情報判定器に送信するカード読み取り装置と、上記カード読み取り装置に設けられ、認証カードが上記カード読み取り装置に挿入された際に電気を供給する電源供給器とを備えたことを特徴とする端末のアクセス制御装置。

【請求項 9】 端末を使用しようとする際に、予め登録

してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって、上記認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、利用者の使用時間を登録し、その使用時間を過ぎた利用者については、上記端末使用許可情報記録器へ端末使用許可情報を記録するのを禁止するタイマーとを備えたことを特徴とする認証カード。

【請求項10】 端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードであって、上記認証カードは、利用者自体の指紋を読み取る指紋読み取り器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報が記録される端末使用許可情報記録器と、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、利用者の使用回数を登録し、その使用回数を過ぎた利用者については、上記端末使用許可情報記録器へ端末使用許可情報を記録するのを禁止するカウンタとを備えたことを特徴とする認証カード。

【請求項11】 カード読み取り装置に設けられ、端末使用許可情報を判定し、正しい情報であった場合、端末に使用許可情報を送信し、端末を使用可能にする端末使用許可情報判定器と、端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードと、上記認証カードに設けられ、利用者自体の指紋を読み取る指紋読み取り器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判定器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報を無線で送信する無線通信器と、上記無線で送信された端末使用許可情報を受信して、上記端末使用許可情報判定器に送信する受信器を備えたことを特徴とする端末のアクセス制御装置。

【請求項12】 カード読み取り装置に設けられ、端末使用許可情報を判定し、正しい情報であった場合、端末に使用許可情報を送信し、端末を使用可能にする端末使用許可情報判定器と、端末を使用しようとする際に、予め登録してある指紋情報と利用者自体の指紋が一致した場合に、端末使用許可情報を記録する認証カードと、上記認証カードに設けられ、利用者自体の指紋を読み取る指紋読み取り器と、上記認証カードに設けられ、上記指紋読み取り器が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを判定する指紋情報判

定器と、上記読み取った指紋と登録された指紋情報が一致した場合、端末使用許可情報を赤外線で送信する送信器と、上記赤外線で送信された端末使用許可情報を受信して、端末使用許可情報判定器に送信する受信器とを備えたことを特徴とする端末のアクセス制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は端末に接続し、端末を使用する際に、端末を使用する資格がない利用者であった場合、端末を使用できないようにする端末のアクセス制御装置および認証カードに関するものである。

【0002】

【従来の技術】まず、従来における不正な利用者による端末の使用を制限する端末のアクセス制御について説明する。図13において、1は端末であり、利用者は端末を利用して情報の検索等の作業を行う。2はキーボードであり、端末1に接続されている。3は利用者情報判定器であり、端末1に内蔵され、利用者がキーボード2から入力した情報から、その利用者が端末を使用する資格のある利用者であるかどうかを判定する。ここで利用者が端末1を使用する場合について説明する。利用者が端末1を使用する場合、利用者は端末1に接続されたキーボード2を使用して、登録された利用者名であるLOGIN名と、正しい利用者であることを示すための秘密情報であるPASSWORDを入力する。端末1に内蔵された利用者情報判定器3は、入力されたLOGIN名とPASSWORDが正しく登録されたものであるかを判定し、正しければ利用者に端末1の使用を許可する。

【0003】しかし、LOGIN名とPASSWORDは、不正な利用者によって知られた場合、端末が不正に使用される危険がある。また、利用者がLOGIN名やPASSWORDを忘れてしまった場合、端末を使用できなくなる可能性もある。そこで、図14に示すような磁気カードを利用したり、図15に示すような端末の利用許可情報が書き込まれた集積回路を組み込んだカードを利用したり、図16に示すような指紋判定器を利用したりして、LOGIN名とPASSWORDが、不正な利用者によって知られないようにしたり、又、LOGIN名やPASSWORDを忘れてしまった場合、端末が使用できなくなるということを防いでいる。

【0004】図14は磁気カードを利用したアクセス制御を説明する図であって、図において4は磁気カードであり、端末1を利用する利用者が所持し、端末1を使用する場合に、端末1に接続されたカード読み取り装置6に挿入する。5は端末使用許可情報が書き込まれた磁気テープであり、磁気カード4に組み込まれていて、端末1の使用を許可するための情報が書き込まれている。6はカード読み取り装置であり、端末に接続され、利用者が端末1を利用しようとする場合、利用者が所持している磁気カード4を挿入し、磁気カード4に組み込まれ

た、端末使用許可情報が書き込まれた磁気テープ 5 から端末使用許可情報を読み取る。7 は端末使用許可情報判定器であり、カード読み取り装置 6 に内蔵され、カード読み取り装置 6 が読み取った、磁気カード 4 の端末使用許可情報を判定し、情報が正しかった場合、端末 1 の使用を許可するための情報を端末 1 に送信する。

【0 0 0 5】次に動作について説明する。まず、利用者が端末 1 を使用する場合、所持している磁気カード 4 の端末使用許可情報が書き込まれた磁気テープ 5 が組み込まれた側をカード読み取り装置 6 に挿入する。カード読み取り装置 6 は、磁気カード 4 に組み込まれた端末使用許可情報が書き込まれた磁気テープ 5 から、端末使用許可情報を読み取る。カード読み取り装置 6 が、読み取った端末使用許可情報を、カード読み取り装置 6 に内蔵された端末使用許可情報判定器 7 が正しい情報であるかどうか判定し、正しい情報であれば、端末 1 の使用を許可するための情報を端末 1 に送信する。端末 1 はカード読み取り装置 6 に内蔵された端末使用許可情報判定器 7 から送信された使用を許可するための情報を受信し、利用者に対して端末を使用可能にする。カード読み取り装置 6 が読み取った情報が正しい情報でなかった場合には、端末使用許可情報判定器 7 は端末 1 の使用を許可するための情報を端末 1 に送信しない。従って、端末 1 は使用可能にならないため、利用者は使用することができない。

【0 0 0 6】図 1 5 は集積回路を組み込んだカードを利用したアクセス制御を説明する図であって、図において 7 は図 1 4 と同じである。8 は集積回路を組み込んだカードであり、端末 1 を利用する利用者が所持し、端末 1 を使用する場合に、端末 1 に接続されたカード読み取り装置 1 0 に挿入する。9 は端末使用許可情報が書き込まれた集積回路であり、集積回路を組み込んだカード 8 に組み込まれていて、端末 1 の使用を許可するための情報が書き込まれている。1 0 はカード読み取り装置であり、端末 1 に接続され、利用者が端末 1 を利用しようとする場合、利用者が所持している集積回路を組み込んだカード 8 を挿入し、集積回路を組み込んだカード 8 に組み込まれた、端末使用許可情報が書き込まれた集積回路 9 から端末使用許可情報を読み取る。

【0 0 0 7】次に動作について説明する。まず、利用者が端末 1 を使用する場合、所持している集積回路を組み込んだカード 8 の端末使用許可情報が書き込まれた集積回路 9 が組み込まれた側をカード読み取り装置 1 0 に挿入する。カード読み取り装置 1 0 は、集積回路を組み込んだカード 8 に組み込まれた端末使用許可情報が書き込まれた集積回路 9 から、端末使用許可情報を読み取る。カード読み取り装置 1 0 が、読み取った端末使用許可情報を、カード読み取り装置 1 0 に内蔵された端末使用許可情報判定器 7 が正しい情報であるかどうか判定し、正しい情報であれば、端末 1 の使用を許可するための情報

を端末 1 に送信する。端末 1 はカード読み取り装置 1 0 に内蔵された端末使用許可情報判定器 7 から送信された使用を許可するための情報を受信し、利用者に対して端末を使用可能にする。カード読み取り装置 1 0 が読み取った情報が正しい情報でなかった場合には、端末使用許可情報判定器 7 は端末 1 の使用を許可するための情報を端末 1 に送信しない。従って、端末 1 は使用可能にならないため、利用者は使用することができない。

【0 0 0 8】図 1 6 は指紋認証装置を利用したアクセス制御を説明する図であって、図において 1 1 は指紋認証装置であり、端末 1 に接続され、利用者が端末 1 を使用する場合に、利用者が指紋を押し付ける。1 2 は指紋読み取り器であり、指紋認証装置 1 2 に組み込まれていて、利用者が押し付けた指紋を読み取る。1 3 は指紋判定器であり、指紋読み取り器 1 2 が読み取った利用者の指紋情報と複数の指紋の情報を記憶するメモリ 1 4 に記憶された指紋の情報が一致するかどうかを判定し、一致した場合、端末 1 の使用を許可するための情報を端末 1 に送信する。1 4 は複数の指紋の情報を記憶するメモリであって、端末 1 を使用できる複数の利用者の指紋の情報が記憶されている。

【0 0 0 9】次に動作について説明する。まず、利用者が端末 1 を使用する場合、利用者の指紋を、指紋認証装置 1 1 に組み込まれた指紋読み取り器 1 2 に押し付ける。指紋読み取り器 1 2 は、押し付けられた利用者の指紋の情報を読み取る。指紋読み取り器 1 2 が読み取った利用者の指紋の情報を、指紋認証装置 1 1 に内蔵された指紋判定器 1 3 が、同じく指紋認証装置 1 1 に内蔵された複数の指紋の情報を記憶するメモリ 1 4 に記憶された、端末の使用を許可する利用者の指紋の情報と比較する。指紋判定器 1 3 は、指紋読み取り器 1 2 が読み取った指紋の情報が複数の指紋の情報を記憶するメモリ 1 4 に記憶された指紋の情報と一致した場合、端末 1 の使用を許可するための情報を端末 1 に送信する。端末 1 は指紋認証装置 1 1 から送信された使用を許可するための情報を受信し、利用者に対して端末を使用可能にする。一方、指紋読み取り器 1 2 が読み取った指紋の情報が複数の指紋の情報を記憶するメモリ 1 4 に記憶された指紋の情報と一致しなかった場合には、指紋判定器 1 3 は端末 1 の使用を許可するための情報を端末 1 に送信しない。従って、端末 1 は使用可能にならないため、利用者は使用することができない。

【0 0 1 0】

【発明が解決しようとする課題】従来の端末のアクセス制御装置は、上記のように端末の使用を制限していた。しかし、磁気カードや集積回路を組み込んだカードによってアクセス制御を行う方法では、磁気カードや集積回路を組み込んだカードを利用者が紛失し、不正な利用者によって使用される可能性があった。一方、利用者の指紋を利用してアクセス制御を行う方法では、利用者が増

えたり、減ったり、あるいは変更があった場合、端末に接続された全ての指紋認証装置の設定を変更する必要がある。端末の台数が少ない場合は、変更作業も容易だが、端末の台数が増えた場合は、変更作業は繁雑になる。

【0011】この発明は上記のような問題点を解消するためになされたもので、利用者の指紋とカード式の認証装置に登録された指紋情報が一致した場合に、端末使用許可情報を記入することで、不正な利用者が利用することを防ぎ、又、利用者の増減があった場合にも、個々の端末に接続された読み取り装置の設定を変更せずに済むようにすることを目的とする。

【0012】

【課題を解決するための手段】第1の発明による端末のアクセス制御装置は、利用者の指紋を認識し、正しい利用者であった場合に、端末使用許可情報記入器に、端末使用許可情報を記入し、その情報をカード読み取り装置が読み取るようにすることで、カード式認証装置が不正な利用者の手に渡った場合でも、不正な利用者が端末を利用できないようにする。

【0013】第2の発明による認証カードは、複数の指紋の情報を記憶するためのメモリを備えることで、複数の利用者が同じ認証カードを利用できるようにする。

【0014】第3の発明による認証カードは、認証カードが不正な利用者に使用されている場合、不正な利用者が端末を使用できないだけでなく、端末が不正に使用されようとしているという事実を離れた場所に知らせることができるようにする。

【0015】第4の発明による認証カードは、認証カードが不正な利用者に使用されている場合、無線で通信又は音を出すことによって、不正な利用者が端末を使用できないだけでなく、端末が不正に使用されようとしているという事実を周囲に知らせることができるようにする。

【0016】第5の発明による認証カードは、外部電源から電気を供給できるようにすることで、内部電源に充電できるようにする。

【0017】第6の発明による認証カードは、太陽電池を使用することで、太陽電池の部分に光が当たれば、内部電源に電気を供給できるようにする。

【0018】第7の発明による認証カードは、振動により発電する発電器を備えることで、認証カードを振動させれば、内部電源に電気を供給できるようにする。

【0019】第8の発明による端末のアクセス制御装置は、カード読み取り装置から電気の供給を受けることができるようにすることで、内部電源がなくても認証カードが利用できるようにする。

【0020】第9の発明による認証カードは、使用時間を記憶するタイマーを備えることで、利用者の使用時間が過ぎた場合、認証カードが使用できないようにする。

【0021】第10の発明による認証カードは、使用回数を記憶するカウンターを備えることで、利用者の使用回数が過ぎた場合、認証カードが使用できないようにする。

【0022】第11の発明による端末のアクセス制御装置は、利用者の指紋を認識し、正しい利用者であった場合に、端末使用許可情報を無線を使用して送信することで、端末から離れた場所から、利用者が正しい利用者かどうかを認証することができるようにする。

【0023】第12の発明による端末のアクセス制御装置は、利用者の指紋を認識し、正しい利用者であった場合に、端末使用許可情報を赤外線を使用して送信することで、端末から離れた場所から、利用者が正しい利用者かどうかを認証することができるようにする。

【0024】

【発明の実施の形態】

実施の形態1. 図1は、この発明の実施の形態1を示す図であり、図において1、7は図15と同じである。15はカード式認証装置（認証カード）であって、端末1を使用する利用者は、指紋を押し付けて、カード読み取り装置20に挿入する。16は指紋読み取り器であって、カード式認証装置15に組み込まれていて、利用者が押し付けた指紋を読み取る。17は端末使用許可情報記入器であって、カード式認証装置15に組み込まれており、指紋読み取り器16が読み取った指紋情報と、登録された利用者の指紋情報が一致するかどうかを指紋情報判定器18が判定し、一致した場合に端末使用許可情報が書き込まれる。18は指紋情報判定器であって、カード式認証装置15に内蔵されており、登録してある指紋情報と、指紋読み取り器16が読み取った利用者の指紋情報とが一致するかどうかを判定し、一致した場合には、端末使用許可情報記入器17に端末使用許可情報を書き込む。19は内部電源であって、カード式認証装置15に電気を供給する。20はカード読み取り装置であり、端末1に接続され、利用者が端末1を利用しようとする場合、利用者が所持しているカード式認証装置15を挿入し、カード式認証装置15に組み込まれた、端末使用許可情報記入器17から端末使用許可情報を読み取る。

【0025】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置15の持ち主である利用者が端末1を使用する場合、利用者はカード式認証装置15に組み込まれている指紋読み取り器16に自分の指紋を押し付ける。指紋読み取り器16は利用者の指紋を読み取り、カード式認証装置15に内蔵されている指紋情報判定器18に読み取った情報を送る。指紋情報判定器18は送られた情報が登録されている指紋情報と一致するかを判定する。この場合は、カード式認証装置15の持ち主である利用者であるため、送られた情報と登録されている指

紋情報は一致し、カード式認証装置 15 に組み込まれている端末使用許可情報記入器 17 に端末使用許可情報が書き込まれる。指紋読み取り器 16、端末使用情報記入器 17、指紋情報判定器 18 は、それぞれ、カード式認証装置 15 に内蔵された内部電源 19 から電気を供給されている。

【0026】利用者は自分の指紋をカード式認証装置 15 に押し付けた後、カード読み取り装置 20 に、端末使用情報記入器 17 が組み込まれた側を挿入する。カード読み取り装置 20 は、端末使用情報記入器 17 から端末使用許可情報を読み取る。カード読み取り装置 20 が、読み取った情報を、カード読み取り装置 20 に内蔵された端末使用許可情報判定器 7 が正しい情報であるかどうかを判定する。この場合は正しい情報であるので、端末 1 の使用を許可するための情報を端末 1 に送信する。端末 1 は端末使用許可情報判定器 7 から送信された使用を許可するための情報を受信し、利用者に対して端末を使用可能にする。

【0027】次に、カード式認証装置 15 の持ち主でない利用者がカード式認証装置 15 を使用した場合、指紋読み取り器 16 は利用者の指紋を読み取り、カード式認証装置 15 に内蔵されている指紋情報判定器 18 に読み取った情報を送る。この場合は、カード式認証装置 15 の持ち主でないため、送られた情報と登録されている指紋情報は一致せず、カード式認証装置 15 に組み込まれている端末使用許可情報記入器 17 に端末使用許可情報が書き込まれない。その後、利用者はカード読み取り装置 20 に、端末使用情報記入器 18 が組み込まれた側を挿入する。カード読み取り装置 20 は、端末使用情報記入器 18 から端末使用許可情報を読み取る。カード読み取り装置 20 が、読み取った情報を、カード読み取り装置 20 に内蔵された端末使用許可情報判定器 7 が正しい情報であるかどうかを判定する。この場合は正しくない情報であるので、端末 1 の使用を許可するための情報は端末 1 に送信されず、利用者は端末を使用することができない。このようにして、カード式認証装置の持ち主以外の利用者が、端末を使用するのを防ぐことを可能にする。

【0028】実施の形態 2。図 2 は、この発明の実施の形態 2 を示す図であり、図において 15～19 は図 1 と同じである。21 は複数の指紋情報を記憶するメモリであって、カード式認証装置 15 に内蔵されており、複数の利用者の指紋情報を記憶している。

【0029】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置 15 の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置 15 に組み込まれている指紋読み取り器 16 に自分の指紋を押し付ける。指紋読み取り器 16 は利用者の指紋を読み取り、カード式認証装置 15 に内蔵されている指紋情報判定器 18 に

読み取った情報を送る。指紋情報判定器 18 は送られた情報がカード式認証装置 15 に内蔵されている複数の指紋の情報を記憶するメモリ 21 に登録されている複数の指紋情報のうちのひとつと一致するかを判定する。この場合は、カード式認証装置 15 の持ち主である利用者であるため、送られた情報と登録されている指紋情報は一致し、カード式認証装置 15 に組み込まれている端末使用許可情報記入器 17 に端末使用許可情報が書き込まれる。指紋読み取り器 16、端末使用情報記入器 17、指紋情報判定器 18、複数の指紋の情報を記憶するメモリ 21 は、それぞれ、カード式認証装置 15 に内蔵された内部電源 19 から電気を供給されている。

【0030】また、カード式認証装置 15 の持ち主である他の利用者が、情報検索等の作業を行うために端末の使用する場合、利用者はカード式認証装置 15 に組み込まれている指紋読み取り器 16 に自分の指紋を押し付ける。指紋読み取り器 16 は利用者の指紋を読み取り、カード式認証装置 15 に内蔵されている指紋情報判定器 18 に読み取った情報を送る。指紋情報判定器 18 は送られた情報がカード式認証装置 15 に内蔵されている複数の指紋の情報を記憶するメモリ 21 に登録されている複数の指紋情報のうちのひとつと一致するかを判定する。この場合も、カード式認証装置 15 の持ち主である利用者であるため、送られた情報と登録されている指紋情報は一致し、指紋情報判定器 18 は端末使用許可情報記入器 17 に端末使用許可情報を書き込む。このようにして、複数の利用者が同じカード式認証装置を使用することを可能にする。

【0031】実施の形態 3。図 3 は、この発明の実施の形態 3 を示す図であり、図において 15～19 は図 1 と同じである。22 は不正利用された事を無線で送信する無線通信器であって、カード式認証装置 15 に組み込まれており、指紋読み取り器 16 が読み取った利用者の指紋情報が、指紋情報判定器 18 に登録された利用者の指紋情報と一致しなかった場合、正規の利用者でない人物が端末を使用しようとしているという情報を無線で送信する。23 は無線通信器からの情報を受信する受信器であって、不正利用された事を無線で送信する無線通信器 22 から、正規の利用者でない人物がカード式認証装置 15 を使用しようとしているという情報を無線で受信する。

【0032】次に動作について説明する。例えば、カード式認証装置 15 の持ち主でない利用者が端末を使用しようとする場合、利用者はカード式認証装置 15 に組み込まれている指紋読み取り器 16 に自分の指紋を押し付ける。指紋読み取り器 16 は利用者の指紋を読み取り、カード式認証装置 15 に内蔵されている指紋情報判定器 18 に読み取った情報を送る。指紋情報判定器 18 は送られた情報と登録されている指紋情報とが一致するかを判定する。この場合は、カード式認証装置 15 の持ち主

でない利用者であるため、送られた情報と登録されている指紋情報は一致しない。従って、指紋情報判定器 1 8 は、カード式認証装置 1 5 に組み込まれている不正利用された事を無線で送信する無線通信器 2 2 に、正規の利用者でない利用者がカード式認証装置 1 5 を使用しているという情報を送る。不正利用された事を無線で送信する無線通信器 2 2 は、受信した情報を無線で送信する。無線通信器からの情報を受信する受信器 2 3 は、カード式認証装置 1 5 に組み込まれた無線通信器 2 2 から、正規の利用者でない利用者がカード式認証装置 1 5 を使用しているという情報を受信する。指紋読み取り器 1 6、端末使用情報記入器 1 7、指紋情報判定器 1 8、不正利用された事を無線で送信する無線通信器 2 2 は、それぞれ、カード式認証装置 1 5 に内蔵された内部電源 1 9 から電気を供給されている。このようにして、正規の利用者でない人物が端末を使用しようとしているという情報を、離れた場所で知ることを可能にする。

【0033】実施の形態 4. 図 4 は、この発明の実施の形態 4 を示す図であり、図において 1 5 ~ 1 9 は図 1 と同じである。2 4 は不正利用された事を音で知らせるスピーカーであって、カード式認証装置 1 5 に組み込まれており、指紋読み取り器 1 6 が読み取った利用者の指紋情報が、指紋情報判定器 1 8 に登録された利用者の指紋情報と一致しなかった場合、正規の利用者でない人物がカード式認証装置 1 5 を使用しようとしているという情報を音で周りに知らせる。

【0034】次に動作について説明する。例えば、カード式認証装置 1 5 の持ち主でない利用者が端末を使用しようとする場合、利用者はカード式認証装置 1 5 に組み込まれている指紋読み取り器 1 6 に自分の指紋を押し付ける。指紋読み取り器 1 6 は利用者の指紋を読み取り、カード式認証装置 1 5 に内蔵されている指紋情報判定器 1 8 に読み取った情報を送る。指紋情報判定器 1 8 は送られた情報と登録されている指紋情報とが一致するかを判定する。この場合は、カード式認証装置 1 5 の持ち主でない利用者であるため、送られた情報と登録されている指紋情報は一致しない。従って、指紋情報判定器 1 8 は、カード式認証装置 1 5 に組み込まれている不正利用された事を音で知らせるスピーカー 2 4 に、正規の利用者でない利用者がカード式認証装置 1 5 を利用しているという信号を送る。不正利用された事を音で知らせるスピーカー 2 4 は、受信した信号によって、音を発生し、正規の利用者でない利用者がカード式認証装置 1 5 を使用しているということを周囲に知らせる。指紋読み取り器 1 6、端末使用情報記入器 1 7、指紋情報判定器 1 8、不正利用された事を音で知らせるスピーカー 2 4 は、それぞれ、カード式認証装置 1 5 に内蔵された内部電源 1 9 から電気を供給されている。このようにして、正規の利用者でない人物が端末を使用しようとしているという情報を、周囲の人間が知ることを可能にする。

【0035】実施の形態 5. 図 5 は、この発明の実施の形態 5 を示す図であり、図において 1 5 ~ 1 9 は図 1 と同じである。2 5 は外部から供給された電気によって内部電源を充電する充電器であって、カード式認証装置 1 5 に内蔵されており、外部から電気を供給する電源装置 2 6 から、電気を供給を受けて内部電源 1 9 の充電を行う。2 6 は外部から電気を供給する電源装置であって、外部から供給された電気によって内部電源を充電する充電器 2 5 に電気を供給する。

【0036】次に動作について説明する。例えば、カード式認証装置 1 5 に内蔵された内部電源 1 9 の電気が残り少なくなり、指紋読み取り器 1 6、端末使用情報記入器 1 7、指紋情報判定器 1 8 が機能しなくなった際、外部から電気を供給する電源装置 2 6 を使用して、外部から供給された電気によって内部電源を充電する充電器 2 5 に電気を供給する。外部から供給された電気によって内部電源を充電する充電器 2 5 は供給された電気を、カード式認証装置 1 5 に内蔵された内部電源 1 9 に電気を供給する。内部電源 1 9 に電気が供給されることで、指紋読み取り器 1 6、端末使用情報記入器 1 7、指紋情報判定器 1 8 を再び機能させることが可能になる。このようにして、内部電源の電気が少なくなっても、外部から供給することで、再びカード式認証装置を利用可能にする。

【0037】実施の形態 6. 図 6 は、この発明の実施の形態 6 を示す図であり、図において 1 5 ~ 1 9 は図 1 と同じである。2 7 は太陽電池であって、カード式認証装置 1 5 に組み込まれており、外部からの光によって発電を行い、内部電源 1 9 に電気を供給する。

【0038】次に動作について説明する。例えば、カード式認証装置 1 5 に光を当てることによって、カード式認証装置 1 5 に組み込まれた太陽電池 2 7 が発電し、カード式認証装置 1 5 に内蔵された内部電源 1 9 に電気を供給する。このようにして、光を当てることで、カード式認証装置に電気を供給することを可能にする。

【0039】実施の形態 7. 図 7 は、この発明の実施の形態 7 を示す図であり、図において 1 5 ~ 1 9 は図 1 と同じである。2 8 は振動によって発電する振動発電器であって、カード式認証装置 1 5 に内蔵されており、カード式認証装置 1 5 を振動させることによって発電を行い、内部電源 1 9 に電気を供給する。

【0040】次に動作について説明する。例えば、カード式認証装置 1 5 を振動させることによって、カード式認証装置 1 5 に組み込まれた振動によって発電する振動発電器 2 8 が発電し、カード式認証装置 1 5 に内蔵された内部電源 1 9 に電気を供給する。このようにして、振動させることによって、カード式認証装置に電気を供給することを可能にする。

【0041】実施の形態 8. 図 8 は、この発明の実施の形態 8 を示す図であり、図において 7、1 5 ~ 1 8、2

0は図1と同じである。29はカード読み取り装置から電源を供給する外部電源器であって、カード式認証装置15に組み込まれており、カード式認証装置15がカード読み取り装置20に挿入された時に、カード読み取り装置20に内蔵された電源供給器30から電気を供給される。30は電源供給器であって、カード読み取り装置20に組み込まれており、カード式認証装置15が挿入された時に、カード式認証装置15に電気を供給する。

【0042】次に動作について説明する。例えば、カード式認証装置15の利用者がカード式認証装置15に組み込まれた指紋読み取り器16に指紋を押し付けたまま、カード式認証装置15をカード読み取り装置20に挿入する。カード読み取り装置20に組み込まれた電源供給器30は、カード式認証装置15が挿入された際、カード式認証装置15に組み込まれたカード読み取り装置20から電源を供給する外部電源器29に電気を供給する。電気を供給されたカード読み取り装置20から電源1を供給する外部電源器29は、指紋読み取り器16、端末使用情報記入器17、指紋情報判定器18に電気を供給する。このことにより、指紋読み取り器16が利用者の指紋を読み取り、指紋情報判定器18が正しい利用者の指紋情報であるかを判断し、端末使用情報記入器17に端末使用許可情報を書き込む。端末使用情報記入器17に書き込まれた端末使用許可情報をカード読み取り装置20が読み取り、カード読み取り装置20に内蔵された端末使用許可情報判定器7が正しい情報であるかどうかを判定する。正しい情報であった場合、カード読み取り装置20に内蔵された端末使用許可情報判定器7は、端末の使用を許可する情報を端末に送信し、利用者は端末を使用することができる。このようにして、カード式認証装置本体に電源がなくても、カード式認証装置を利用可能にする。

【0043】実施の形態9。図9は、この発明の実施の形態9を示す図であり、図において15～19は図1と同じである。31は使用時間を記憶するタイマーであって、カード式認証装置15に内蔵されており、使用時間を記憶し、予め登録された使用時間が過ぎた場合、端末使用許可情報記入器17に、端末使用許可情報が書き込めないようにする。

【0044】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置15の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置15に組み込まれている指紋読み取り器16に自分の指紋を押し付ける。指紋読み取り器16は利用者の指紋を読み取り、カード式認証装置15に内蔵されている指紋情報判定器18に読み取った情報を送る。指紋情報判定器18は送られた情報と登録されている指紋情報と一致するかを判定する。同時に、使用時間を記憶するタイマー31が、カード式認証装置15の使用時間をチェックする。利用者の

使用時間が使用時間を記憶するタイマー31に記憶された使用時間を過ぎていた場合、カード式認証装置15に組み込まれている端末使用許可情報記入器17に端末使用許可情報が書き込めないようにする。この場合、利用者の指紋と登録されている指紋情報は一致しても、カード式認証装置15は使用できない。このようにして、カード式認証装置の使用時間を決めておき、使用時間を過ぎた利用者がカード式認証装置を利用することを不可能にする。

【0045】実施の形態10。図10は、この発明の実施の形態10を示す図であり、図において15～19は図1と同じである。32は使用回数をカウントするカウンタであって、カード式認証装置16に内蔵されており、使用回数をカウントし、予め登録された使用回数が過ぎた場合、端末使用許可情報記入器17に、端末使用許可情報が書き込めないようにする。

【0046】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置15の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置15に組み込まれている指紋読み取り器16に自分の指紋を押し付ける。指紋読み取り器16は利用者の指紋を読み取り、カード式認証装置15に内蔵されている指紋情報判定器18に読み取った情報を送る。指紋情報判定器18は送られた情報と登録されている指紋情報と一致するかを判定する。同時に、使用回数をカウントするカウンタ32が、カード式認証装置15の使用回数のカウントを行い、予め登録された使用回数とのチェックを行う。利用者の使用回数が使用回数をカウントするカウンタ32に記憶された使用回数を過ぎていた場合、カード式認証装置15に組み込まれている端末使用許可情報記入器17に端末使用許可情報が書き込めないようにする。この場合、利用者の指紋と登録されている指紋情報は一致しても、カード式認証装置15は使用できない。このようにして、カード式認証装置の使用回数を決めておき、使用回数を過ぎた利用者がカード式認証装置を利用することを不可能にする。

【0047】実施の形態11。図11は、この発明の実施の形態11を示す図であり、図において7、15、16、18、19は図1と同じである。33は端末使用許可情報を無線で送信する無線通信器であって、カード式認証装置15に内蔵されており、端末使用許可情報を無線で送信する。34は端末使用許可情報を無線で受信する受信器であって、端末使用許可情報を受信する。

【0048】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置15の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置15に組み込まれている指紋読み取り器16に自分の指紋を押し付ける。指紋読み取り器16は利用者の指紋を読み取り、カード

式認証装置15に内蔵されている指紋情報判定器18に読み取った情報を送る。指紋情報判定器18は送られた情報と登録されている指紋情報とが一致するかを判定し、一致した場合、端末使用許可情報をカード式認証装置15に組み込まれている端末使用許可情報を無線で送信する無線通信器22に送信する。端末使用許可情報を無線で送信する無線通信器32は、指紋情報判定器18から送られた端末使用許可情報を、端末に接続されている端末使用許可情報を無線で受信する受信器34に無線で送信する。端末使用許可情報を無線で受信する受信器34は、端末使用許可情報を受信すると、端末使用許可情報を無線で受信する受信器34に内蔵された端末使用許可情報判定器7に情報を送る。端末使用許可情報を無線で受信する受信器34に内蔵された端末使用許可情報判定器7は、受信した情報が正しい情報であるかどうかを判定し、正しい情報であった場合、端末に使用許可情報を送信する。このようにして、端末から離れた場所から、カード式認証装置を利用して端末を使用することを可能にする。

【0049】実施の形態12. 図12は、この発明の実施の形態12を示す図であり、図において7、15、16、18、19は図1と同じである。35は端末使用許可情報を赤外線で送信する送信器であって、カード式認証装置15に内蔵されており、端末使用許可情報を赤外線で送信する。36は端末使用許可情報を赤外線を受信する受信器であって、端末使用許可情報を受信する。

【0050】次に動作について説明する。例えば、情報検索等の作業を行うために端末の使用を許可された、カード式認証装置15の持ち主である利用者が端末を使用する場合、利用者はカード式認証装置15に組み込まれている指紋読み取り器16に自分の指紋を押し付ける。指紋読み取り器16は利用者の指紋を読み取り、カード式認証装置15に内蔵されている指紋情報判定器18に読み取った情報を送る。指紋情報判定器18は送られた情報と登録されている指紋情報とが一致するかを判定し、一致した場合、端末使用許可情報をカード式認証装置15に組み込まれている端末使用許可情報を赤外線

とを可能にする。

【0051】

【発明の効果】第1の発明によれば、認証カードに、利用者自体の指紋を読み取り、読取られた指紋と登録してある指紋情報が一致した場合、端末の使用許可情報を書き込むことで、認証カードの持ち主以外の利用者が、端末を使用するのを防ぐことができる。

【0052】第2の発明によれば、認証カードに複数の利用者の指紋情報を登録することのできるメモリを内蔵することで、複数の利用者が認証カードを使用することができる。

【0053】第3の発明によれば、認証カードの持ち主でない利用者が、端末を使用しようとしていることを、報知することで、離れた場所で認証カードの持ち主でない人物が、端末を使用しようとしているということを知ることができる。

【0054】第4の発明によれば、認証カードの持ち主でない利用者が、端末を使用しようとしていることを、無線又は音を出して知らせることで、周囲に認証カードの持ち主でない人物が、端末を使用しようとしているということを知らせることができる。

【0055】第5の発明によれば、認証カードが充電することを可能にすることで、内部電源の電気容量が少なくなっても、充電することにより、内部電源の電気容量を回復することができる。

【0056】第6の発明によれば、認証カードに太陽電池を組み込むことで、光を当てることで発電し、認証カードを利用することができる。

【0057】第7の発明によれば、認証カードに振動によって発電する発電器を備えることで、振動によって発電し、認証カードを利用することができる。

【0058】第8の発明によれば、認証カードがカード読み取り装置から電気を供給するようにすることで、認証カードに電源を持たなくても、認証カードを利用することができる。

【0059】第9の発明によれば、認証カードに使用時間を登録することで、その使用時間を過ぎた認証カードの利用者が、認証カードを使用できないようにすることができる。

【0060】第10の発明によれば、認証カードに使用回数を登録することで、その使用回数を過ぎた認証カードの利用者が、認証カードを使用できないようにすることができる。

【0061】第11の発明によれば、端末使用許可情報を無線で送信することで、端末から離れた場所から、認証カードを利用して端末を使用することを可能にする。

【0062】第12の発明によれば、端末使用許可情報を赤外線

【図面の簡単な説明】

- 【図1】 この発明の実施の形態1を示す図である。
 【図2】 この発明の実施の形態2を示す図である。
 【図3】 この発明の実施の形態3を示す図である。
 【図4】 この発明の実施の形態4を示す図である。
 【図5】 この発明の実施の形態5を示す図である。
 【図6】 この発明の実施の形態6を示す図である。
 【図7】 この発明の実施の形態7を示す図である。
 【図8】 この発明の実施の形態8を示す図である。
 【図9】 この発明の実施の形態9を示す図である。
 【図10】 この発明の実施の形態10を示す図である。
 【図11】 この発明の実施の形態11を示す図である。
 【図12】 この発明の実施の形態12を示す図である。
 【図13】 従来の端末におけるアクセス制御を示す図である。
 【図14】 磁気カードを使用した従来のアクセス制御を示す図である。

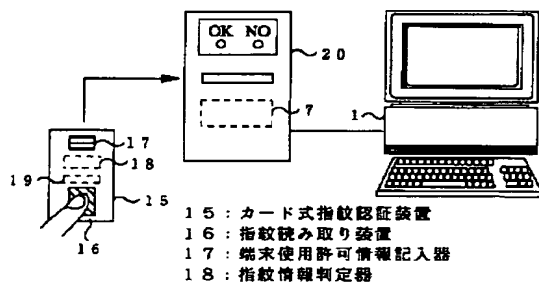
【図15】 集積回路を組み込んだカードを使用した従来のアクセス制御を示す図である。

【図16】 指紋読み取り装置を使用した従来のアクセス制御を示す図である。

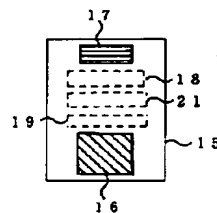
【符号の説明】

- 1 端末、2 キーボード、3 利用者情報判定器、4 磁気カード、5 磁気テープ、6 カード読み取り装置、7 端末使用許可情報判定器、8 カード、9 集積回路、10 カード読み取り装置、11 指紋認証装置、12 指紋読み取り器、13 指紋判定器、14 メモリ、15 カード式指紋認証装置、16 指紋読み取り装置、17 端末使用許可情報記入器、18 指紋情報判定器、19 内部電源、20 カード読み取り装置、21 メモリ、22 無線通信器、23 受信器、24 スピーカー、25 充電器、26 電源装置、27 太陽電池、28 振動発電器、29 外部電源器、30 電源供給器、31 タイマー、32 カウンタ、33 無線通信器、34 受信器、35 送信器、36 受信器。

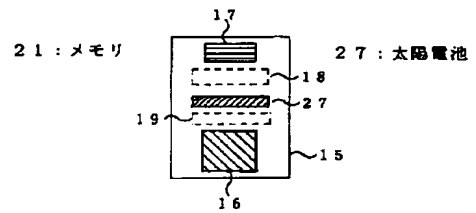
【図1】



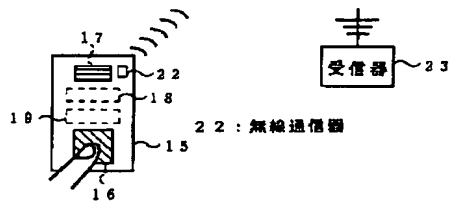
【図2】



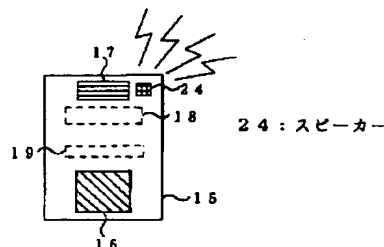
【図6】



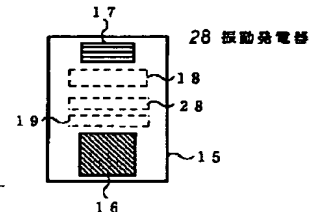
【図3】



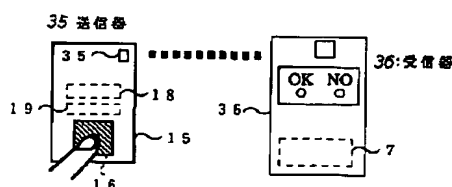
【図4】



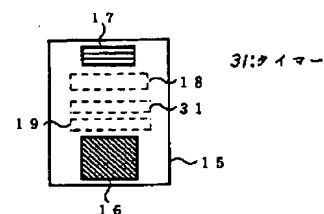
【図7】



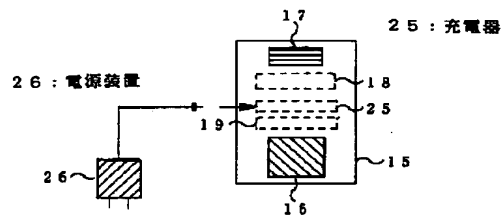
【図12】



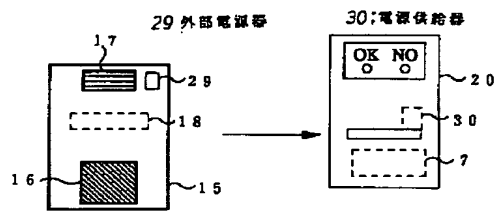
【図9】



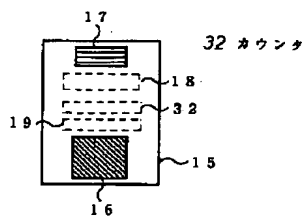
【図5】



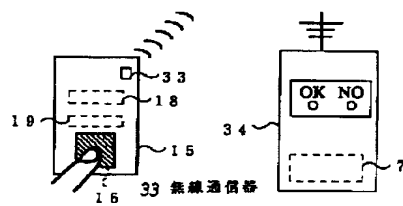
【図8】



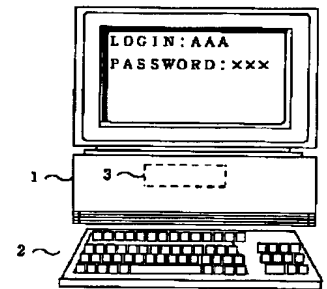
【図10】



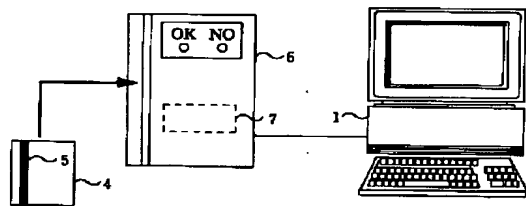
【図11】



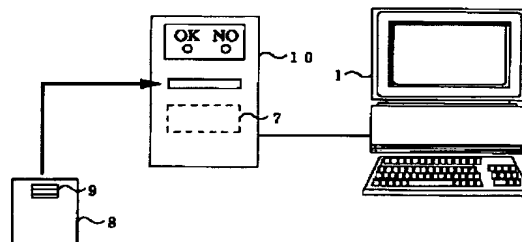
【図13】



【図14】



【図15】



【図16】

